Abstract and Machine Translation obtained from JPO website.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-324219**
(43)Date of publication of application : **08.11.2002**

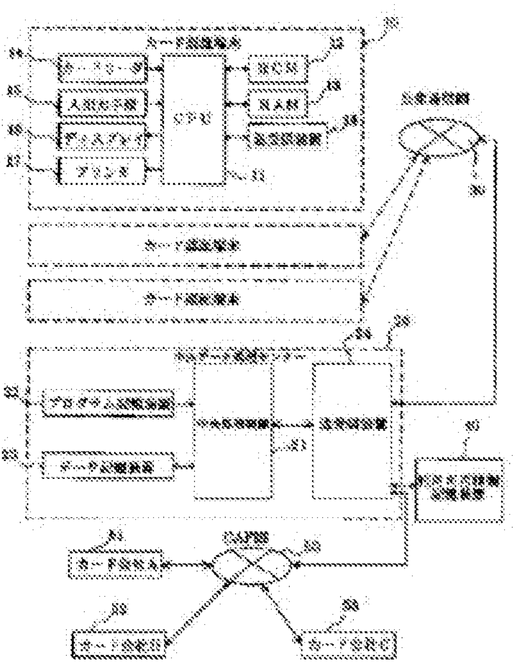
(51)Int.Cl. G06K 17/00
B42D 15/10
G06F 15/00

(21)Application number : **2001-126416**
(22)Date of filing : **24.04.2001**

(71)Applicant : **SEIKO INSTRUMENTS INC**
(72)Inventor : **TACHIBANA HITOSHI**

(54) CARD AUTHENTICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a card authentication system capable of preventing the illegal use of a card due to forgery on a high level.
SOLUTION: This card authentication system is provided with a plurality of card authenticating terminals 10 and a central data processing center 20 connected through a public communication network 30 to those card authenticating terminals so that on-line authentication processing can be executed by the card authenticating terminal 10 by performing access from the central data processing center 20 through a card business integral network system 50 to the respective host computers of card companies 51-53. This card authentication system is provided with a use validity/invalidity information storage device 40 for allowing each card user to preliminarily switch the validity/invalidity of the card, and the on-line authentication is executed only to the card whose use is judged to be valid through the use validity/invalidity storage device 40 by the central data processing center 20.



Machine Translation obtained from JPO website.

[Detailed Description of the Invention]
[0001] [Field of the Invention]this invention -- users, such as a credit card or a debit card, -- it is related with the card authentication system which can prevent an unauthorized use as use being possible only at the time of use of the person himself/herself as the person himself/herself can set up the use propriety of the card concerned.

[0002] [Description of the Prior Art]If a card is published, except for the card which repealed use of a stolen card etc., the card beyond an available limit, etc., a conventional credit card and debit card can always be used in principle, and will become available by Kami who checked the person himself/herself at the time of use.

[0003] [Problem to be solved by the invention]However, after a theft or loss, if a notification can be done promptly, it will be satisfactory, but before a notification is issued, time may be taken, and an unauthorized use cannot be prevented. In the former, it is completely defenseless to the unauthorized use by a counterfeit card.

[0004]This invention makes it problem to provide the card authentication system which can prevent the unauthorized use by forgery highly in view of such a situation.

[0005] [Means for solving problem]The 1st mode of this invention which solves the aforementioned problem Many card authentication terminals, The data processing center connected with these card authentication terminal via a public communication network is provided, In the card authentication system which enabled it to perform on-line authenticating processing at the aforementioned card authentication terminal by accessing each card issuer's host computer on-line via a card business synthesis network system from the aforementioned data processing center, The user of each card has a use propriety information storage device which can change the effective invalidity of the card concerned a priori, and the aforementioned data processing center, It is in the card authentication system performing on-line attestation only to the card judged to be available via the use propriety information storage device concerned.

[0006]The 2nd mode of this invention has the aforementioned use propriety information storage device in the card authentication system receiving the demand to the use good change from the user of a card, and validating use about the card concerned in the 1st mode.

[0007]In the 2nd mode, the 3rd mode of this invention has it in the card authentication system changing into a use failure automatically by predetermined time, after the aforementioned use propriety information storage device receives the demand to the use good change from the user of a card and validates use about the card concerned.

[0008]The 4th mode of this invention has the aforementioned use propriety information storage device in the card authentication system receiving the demand to the use good change from the user of a card via the wireless communication terminal from a user in which 1-3rd modes.

[0009]The 5th mode of this invention has the aforementioned use propriety information storage device in the card authentication system receiving the demand to the use good change from the user of a card via the aforementioned card authentication terminal from the wireless communication terminal from a user in which 1-3rd modes.

[0010]In which 1-5th modes, the aforementioned use propriety information storage device has beforehand data attached to each card, and the 6th mode of this invention has it in the card authentication system registering use propriety about the card registered.

[0011]The 7th mode of this invention has the aforementioned use propriety information storage device in the card authentication system registering only the data about the card which is attached to each card, and which becomes available at any time in which 1-5th modes.

[0012]According to this this invention, the card authentication system which can prevent the unauthorized use by forgery highly can be provided.

[0013] [Mode for carrying out the invention]Hereafter, this invention is explained based on one embodiment.

[0014]The whole one embodiment schematic structure of the credit card authentication system concerning this invention is shown in drawing 1. As shown in drawing 1, many card authentication terminals 10, It is connected via the public communication network 30 of the data processing center 20, and a cable or radio, and the data processing center 20 is connected to the use propriety information storage device 40 and the card business synthesis network 50 via the private telecommunication network. The card business synthesis network 50 has typical CAFIS of card NTT Data, Inc., and connects two or more card issuers 51-53 and financial institutions on-line.

[0015]CPU11 to which the card authentication terminal 10 performs various operations and control, and ROM12 the program was remembered to be, The card reader 14 which can read RAM13 which memorizes various data, and the membership information and card ID of an attestation credit card required, The input output means 15 for inputting information, including a charge, the method of paying, etc., the display 16 which displays an authentication result etc., the printer 17 with which a utilization charge etc. are printed out, and the transceiving equipment 18 for connecting with the public communication network 30 are provided as a main component.

[0016]The central processing unit 21 with which the data processing center 20 performs various operations and control, The program storage 22 the program was remembered to be, the data storage equipment 23 which memorizes various data, and the transceiving equipment 24 for connecting with the public communication network 30, and connecting with the card business synthesis network system 50 are provided as a main component.

[0017]The central processing unit 41 with which the use propriety information storage device 40 performs various operations and control as shown in drawing 2 (a), The program storage 42 the program was remembered to be, and the data storage equipment 43 which memorizes various data, The transceiving equipment 44 for connecting with the data processing center 20 and the acceptance equipment 45 which receives information directly from the communication terminals 60, such as a cellular phone and PHS, are provided, and the use propriety information database 46 is stored in the data storage equipment 43.

[0018]When publishing cards, such as a credit card, as shown in drawing 2 (b) for example, the use propriety information database 46 with a card number, It is the database with which information, for example, a member name, a password, etc. for a user to access were registered, and the information of whether each card is effective or it is invalid is also provided.

[0019]Here, the effective invalid information on the use propriety information database 46 can be changed at any time by a user. Although the method in particular of change by a user is not limited, it may enable it to change it via the web connected via a communication terminal, may enable it to change it by receiving the mail from the communication terminal 60, and may enable it to change it with the spoken command from a communication terminal.

[0020]When an effective invalid change has a validation demand and it has validity and a cancellation demand, may be made to repeal it, but. After it supposes in principle that it is invalid and there is a validation demand, it is preferred that only the predetermined time on short time, such as 2 or 3 minutes, 5 minutes, and 10 etc. minutes, the 1st, etc. cancels only predetermined time automatically, for example after coming into effect. This is for preventing the unauthorized use of a counterfeit card beforehand by coming into effect, only when a user uses.

[0021]As for the acceptance equipment 45, it is preferred to require a predetermined password of accessing, and it may be made to give the addresser notice of a communication terminal a password so that only the validation demand from a regular user may be received and the unjust demand from an unauthorized use person may not be received.

[0022]In order for a user to be able to perform a validation demand easily, preventing such an illegal use, it may be made to transmit by the mail function of a communication terminal for example, with a card number, the password registered beforehand, predetermined membership information, and a validation demand. The application which can perform predetermined encryption processing (one-way operation) to a communication terminal is stored, The result in which predetermined carried out encryption processing using the membership number of a card and the enciphering key registered beforehand is used as a password, and it may be made to transmit this using a mail function with predetermined membership information and a validation demand.

[0023]It may be made to make the number of only an effective card exist in the use propriety information database 46. That is, the acceptance equipment 45 registers into the use propriety information database 46 only the card number received with the validation demand, and when a card number exists in the use propriety information database 46, it presupposes that a card is effective. A password which brings a predetermined result when predetermined encryption processing is performed at the time of card issuing in order to prevent access from an unauthorized use person in this case, For example, if predetermined calculation is performed, as a result publishes a password which always serves as zero and registers only the card number transmitted with such a password, it needs to eliminate unjust registration.

[0024]In the card authentication system explained above, to use a card, the user needs to transmit a validation demand to the acceptance equipment 45 of the use propriety information storage device 40 via communication terminals, such as a cellular phone, beforehand just before use preferably. Then, the user is the card authentication terminal 10 installed in the store or the service counter, and is checked [of whether it is available]. That is, as shown in drawing 3, the card authentication terminal 10 reads membership information and a card number by the card reader 14 (Step S11). This is transmitted to the data processing center 20 via the public communication network 30 from the transceiving equipment 18 (Step S12). If the card information on attestation required is received, the data processing center 20 will ask the use propriety information storage device 40 the use propriety of the card concerned, and will wait for reception of a use propriety decided result (Step S13). The propriety of use of the card concerned is judged from a use propriety decided result (Step S14), and when it cannot use, (Step S14, No), and a use failure are judged as use being impossible to a card authentication terminal (Step S15).

[0025]On the other hand, when available, membership information is separated from the membership information and the card number of (Step S14, Yes), and the received important point authentication card, This is changed into predetermined formatting data, and it transmits to a specific card issuer via the card business synthesis network system 50 (Step S16), and waits for the authentication result from a card issuer (Step S17).

[0026]If the authentication result from a card issuer is received, it will be judged whether an important point authentication card is an invalid card (Step S18), When it is judged as an invalid card (Step S18, Yes), it judges with use being impossible (Step S15), and when it judges that it is not an invalid card, (Step S18 and No) judge that it is effective (Step S19), and transmit the information on the purport that it attests to the card authentication terminal 10 (Step S20). Since processing is the same as processing of the usual credit card and a debit card, explanation omits the data of rental spending, the method of paying, etc.

[0027]Since a user can validate card use only at card utilization time according to the embodiment described above, the unauthorized use of the card by a counterfeit card etc. can be prevented.

[0028]When a user demanded change of the use propriety of a card, made it transmit to the use propriety information storage device 40 directly from the communication terminal 60 in the embodiment described above, but. It is made to transmit to the card authentication terminal 10, and may be made to be transmitted to the use propriety information storage device 40 via the data processing center 20 from the card authentication terminal 10. In this case, it connects automatically, for example and the communication terminal 60 and the card communication terminal 10 may enable it to communicate by radio standards, such as Bluetooth, for example.

[0029]At the embodiment mentioned above, it cannot be overemphasized that it may install in the data processing center 20 although the use propriety information storage device 40 was separately installed in the data processing center 20.

[0030] [Effect of the Invention]As explained above, according to this invention, the effect that the card authentication system which can prevent the unauthorized use by forgery highly can be provided is generated.

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the schematic structure of the card authentication system concerning one embodiment of this invention.
[Drawing 2]It is a figure showing the outline of the use propriety information storage device of this invention.
[Drawing 3]It is a figure showing the procedure of attestation of the card authentication system concerning one embodiment of this invention.
[Explanations of letters or numerals]
10 Card authentication terminal
20 Data processing center
30 Public communication network
40 Use propriety information storage device
50 CAFIS

[Claim(s)]
[Claim 1]In a card authentication system which enabled it to perform on-line authenticating processing at the aforementioned card authentication terminal by having the following and accessing each card issuer's host computer on-line via a card business synthesis network system from the aforementioned data processing center, A user of each card has a use propriety information storage device which can change effective invalidity of the card concerned a priori, and the aforementioned data processing center, A card authentication system performing on-line attestation only to a card judged to be available via the use propriety information storage device concerned.
Many card authentication terminals.
A data processing center connected with these card authentication terminal via a public communication network.

[Claim 2]The card authentication system according to claim 1, wherein the aforementioned use propriety information storage device receives a demand to use good change from a user of a card and validates use about the card concerned.

[Claim 3]The card authentication system according to claim 2 changing the aforementioned use propriety information storage device into a use failure automatically by predetermined time after receiving a demand to use good change from a user of a card and validating use about the card concerned.

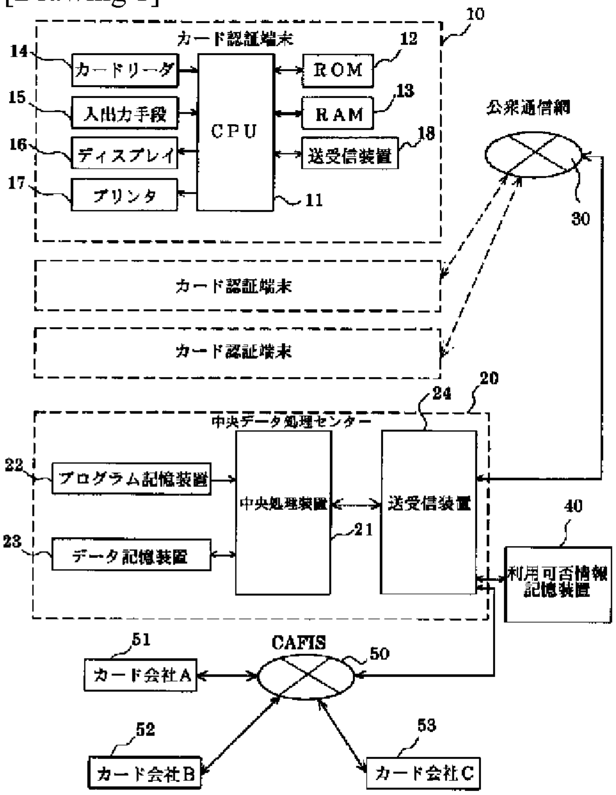
[Claim 4]The card authentication system according to any one of claims 1 to 3, wherein the aforementioned use propriety information storage device receives a demand to use good change from a user of a card via a wireless communication terminal from a user.

[Claim 5]The card authentication system according to any one of claims 1 to 3, wherein the aforementioned use propriety information storage device receives a demand to use good change from a user of a card via the aforementioned card authentication terminal from a wireless communication terminal from a user.

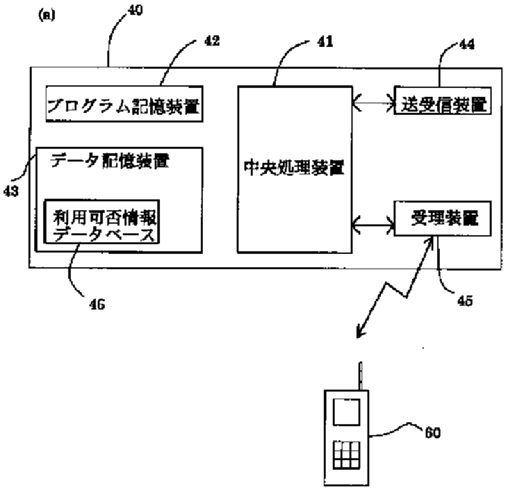
[Claim 6]The card authentication system according to any one of claims 1 to 5, wherein the aforementioned use propriety information storage device registers use propriety about a card which has beforehand data attached to each card, and is registered.

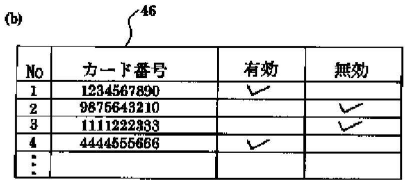
[Claim 7]The card authentication system according to any one of claims 1 to 5, wherein the aforementioned use propriety information storage device registers only data about a card which is attached to each card and which becomes available at any time.

[Drawing 1]


10
カード認証端末
12
14
カードリーダ
CPU
ROM
15
入出力手段
13
RAM
公衆通信網
16
ディスプレイ
18
送受信装置
17
プリンタ
11
30
カード認証端末
カード認証端末
24
20
中央データ処理センター
22
プログラム記憶装置
中央処理装置
送受信装置
40
23
データ記憶装置
21
利用可否情報記憶装置
51
CAFIS
50
カード会社A
52
53
カード会社B
カード会社C

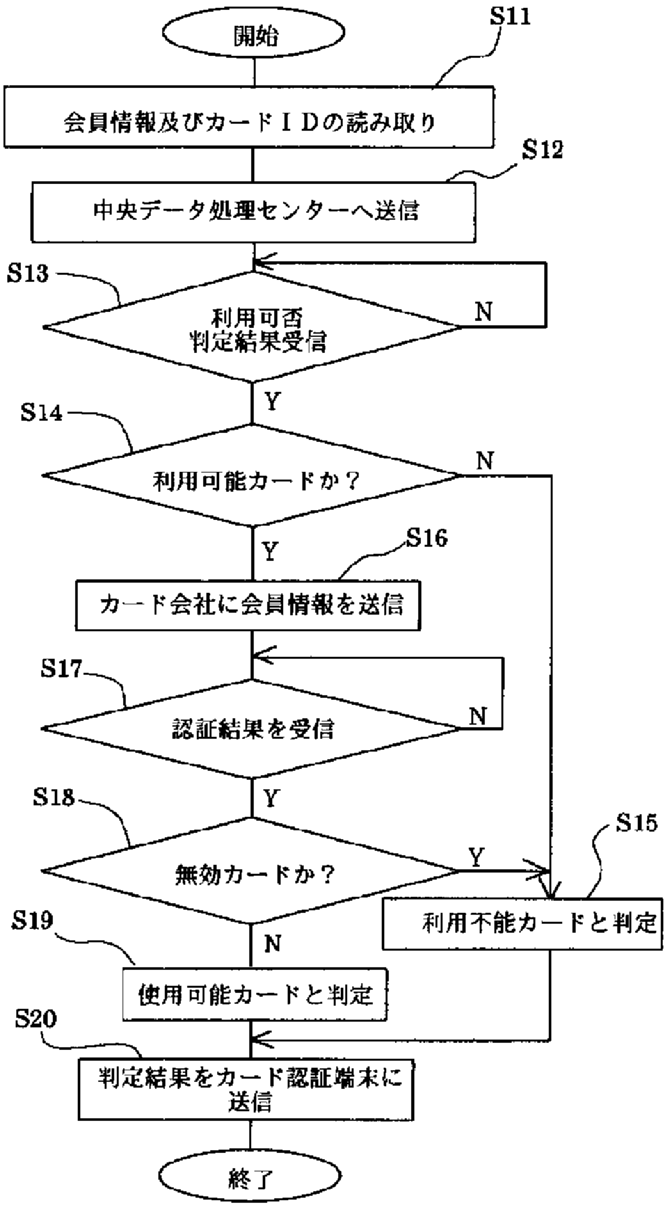
[Drawing 2]


(a)
40
42
41
44
プログラム記憶装置
送受信装置
データ記憶装置
中央処理装置
43
利用可否情報
データベース
受理装置
46
45
60



No	カード番号	有効	無効
1	1234567890	✓	
2	9875643210		✓
3	1111222333		✓
4	4444555666	✓	
⋮			

[Drawing 3]


開始
S11
会員情報及びカードＩＤの読み取り
S12
中央データ処理センターへ送信
S13
利用可否
判定結果受信
N
Y
S14
利用可能カードか？
N
Y
S16
カード会社に会員情報を送信
S17
認証結果を受信
N
Y
S18
無効カードか？
Y
S15
利用不能カードと判定
N
S19
使用可能カードと判定
S20
判定結果をカード認証端末に
送信
終了